

10/579685 17 MAY 2006

Beschreibung

Verfahren zum Zugriff auf eine Datenverarbeitungsanlage

- 5 Die Erfindung betrifft ein Verfahren zum Zugriff auf eine Datenverarbeitungsanlage.

- Nach dem Stand der Technik sind weithin Datenverarbeitungsanlagen bekannt, die aus einer Mehrzahl
10 miteinander zum Datenaustausch vernetzter Datenverarbeitungseinheiten, z. B. Personalcomputer, computergesteuerte Geräte, Server und dgl., bestehen. Dabei ist jeder Datenverarbeitungseinheit eine beschränkte Zahl von Benutzern zugewiesen. Um eine unbefugte Benutzung einer
15 Datenverarbeitungseinheit zu unterbinden, verfügt jeder Benutzer über ein persönliches Passwort. Durch Eingeben des Passworts authentifiziert sich der Benutzer und erhält Zugriff auf die Datenverarbeitungsanlage.
- 20 Insbesondere in Krankenhäusern sind Datenverarbeitungsanlagen heute komplex aufgebaut. Bestandteil solcher Datenverarbeitungsanlagen sind u. a. Diagnose- und Analysegeräte. Derartige Geräte müssen stets in einem einwandfreien Funktionszustand gehalten werden. Insbesondere
25 eine Wartung und eine Reparatur derartiger Geräte erfordert in der Regel einen Zugriff eines Systemtechnikers auf die Datenverarbeitungsanlage. Ein nach wie vor ungelöstes Problem dabei ist, dass damit der Systemtechniker u. U. Zugriff auf personenbezogene Patientendaten erhalten kann. Aus
30 datenschutzrechtlichen Gründen darf ein Zugriff auf eine solche Datenverarbeitungsanlage nur nach dem 4-Augen-Prinzip erfolgen, d. h. nur gleichzeitig durch zwei befugte Personen. In der Praxis lässt sich das allerdings kaum realisieren, weil im Falle einer Funktionsstörung einer
35 Datenverarbeitungsanlage in der Regel eine sofortige Abhilfe erforderlich ist und mitunter zwei befugte und zur Behebung

der Funktionsstörung ausreichend qualifizierte Systemtechniker nicht immer gleichzeitig verfügbar sind.

5 Aus der DE 101 21 819 A1 ist ein Verfahren bekannt, bei dem ein Arzt nur dann Zugriff auf patientenspezifische Daten erhält, wenn der Arzt eine ihm zugewiesene erste Chip-Karte und der gleichzeitig anwesende Patient eine ihm gehörende zweite Chip-Karte in eine beim Arzt befindliche Datenverarbeitungseinrichtung zur Authentifizierung einlesen.

10 Aufgabe der Erfindung ist es, ein Verfahren anzugeben, welches einen eine Datenhoheit eines Systemadministrators sicherstellenden Zugriff auf eine Datenverarbeitungsanlage lediglich nach dem Grundsatz des 4-Augen-Prinzips ermöglicht.

15 Diese Aufgabe wird durch die Merkmale des Anspruchs 1 gelöst. Zweckmäßige Ausgestaltungen des Verfahrens ergeben sich aus den Merkmalen der Ansprüche 2 bis 13.

20 Nach Maßgabe der Erfindung ist ein Verfahren zum Zugriff auf eine Datenverarbeitungsanlage vorgesehen, welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten gebildet ist, mit folgenden Schritten:

25 Bereitstellen eines ersten Authentifizierungsmittels zur Authentifizierung eines Systemadministrators,

30 Authentifizierung des Systemadministrators an einer ersten Datenverarbeitungseinheit durch Übergabe des ersten Authentifizierungsmittels an ein Authentifizierungsprogramm,

Bereitstellen eines zweiten Authentifizierungsmittels zur Authentifizierung eines Systemtechnikers,

35 Authentifizierung des Systemtechnikers an einer zweiten Datenverarbeitungseinheit durch Übergabe des zweiten

Authentifizierungsmittels an das Authentifizierungsprogramm,
und dadurch bedingtes automatisches Erzeugen einer den Träger
des zweiten Authentifizierungsmittels identifizierenden
Identifikationsinformation,

5

Anzeige der Identifikationsinformation an der ersten
Datenverarbeitungseinheit (1) des Systemadministrators und

Freischalten einer Zugangsberechtigung für den
10 Systemtechniker und bedingtes automatisches Auslösen einer
Funktion zum Erzeugen und Speichern einer die Tätigkeit des
Systemtechnikers an der Datenverarbeitungsanlage
protokollierenden Protokolldatei.

15 Nach dem erfindungsgemäßen Verfahren erhält der
Systemtechniker erst nach Übergabe eines ihm zugewiesenen
zweiten Authentifizierungsmittels Zugang zur
Datenverarbeitungsanlage. Die Freischaltung eines solchen
Zugangs wird durch das Erzeugen einer
20 Identifizierungsinformation dokumentiert und an der ersten
Datenverarbeitungseinheit des Systemadministrators
angezeigt. Es wird außerdem eine die Tätigkeit des
Systemtechnikers protokollierende Protokolldatei erzeugt,
anhand derer der Eingriff des Systemtechnikers beispielsweise
25 für den Systemadministrator nachvollzogen werden kann. Damit
ist gewährleistet, dass die Datenhoheit stets der
Systemadministrator inne hat. Anhand der erzeugten
Protokolldateien ist es ihm möglich zu prüfen, ob ein
Systemtechniker unbefugterweise auf Daten zugegriffen hat. In
30 diesem Fall kann der Systemadministrator sofort jeglichen
weiteren Zugang zur Datenverarbeitungsanlage für den
betreffenden Systemtechniker sperren. Mit dem vorgeschlagenen
Verfahren wird ein Zugriff auf eine Datenverarbeitungsanlage
nach dem Grundsatz des 4-Augen-Prinzips ermöglicht. Dabei ist
35 es von besonderem Vorteil, dass ein solcher Zugriff auch dann
erfolgen kann, wenn mit Kenntnis des Systemadministrators

lediglich ein Systemtechniker an einer
Datenverarbeitungseinheit tätig ist.

Unter dem Begriff "Zugriff" wird im Sinne der vorliegenden
5 Erfindung jegliche Tätigkeit verstanden, bei welcher der
Datenbestand einer Datenverarbeitungsanlage gesichtet,
verändert oder ganz oder teilweise kopiert wird. Bei einer
"Datenverarbeitungseinheit" im Sinne der vorliegenden
10 Erfindung handelt es sich um eine Vorrichtung, welche mit
anderen zum Datenaustausch geeigneten Vorrichtungen zum
Datenaustausch verbunden ist. Derartige Vorrichtungen weisen
zum Datenaustausch üblicherweise eine bidirektionale
Schnittstelle auf. Es kann sich dabei um einen
15 Personalcomputer, um computergesteuerte Anlagen oder Geräte
und dgl. handeln.

Unter dem Begriff "Systemadministrator" wird eine Person
verstanden, welche besondere Rechte im Hinblick auf die
Pflege und Wartung der Datenverarbeitungsanlage hat. Der
20 Systemadministrator im Sinne der vorliegenden Erfindung hat
im Gegensatz zu einem Systemtechniker die Möglichkeit, einen
Zugang zur Datenverarbeitungsanlage zu gestatten oder zu
sperren. Diese Möglichkeit wird dem Systemadministrator
insbesondere durch das erste Authentifizierungsmittel
25 zugewiesen.

Zur Authentifizierung des Systemtechnikers kann das zweite
Authentifizierungsmittel mittels des
Authentifizierungsprogramms durch Zugriff auf eine
30 verifizierte zweite Authentifizierungsmittel enthaltende
Datei verglichen und bei Übereinstimmung mit einem der
verifizierten zweiten Authentifizierungsmittel eine
entsprechende Information an den Systemadministrator
übermittelt werden. Unter einem "verifizierten zweiten
35 Authentifizierungsmittel" wird eine Kopie des an den
Systemtechnikers übergebenen zweiten
Authentifizierungsmittels verstanden, welche vom

Systemadministrator in einer nur ihm zugänglichen Datei verwaltet wird. Zum Zugriff auf die Datenverarbeitungsanlage übergibt der Systemadministrator an jeden Systemtechniker ein besonderes zweites Authentifizierungsmittel. Zur

5 Erleichterung der Prüfung der Authentizität der zweiten Authentifizierungsmittel werden diese gemeinsam in der Datei abgelegt. Sofern das Authentifizierungsprogramm feststellt, dass eine Zugriffsanforderung auf der Grundlage eines mit einem verifizierten zweiten Authentifizierungsmittel
10 identischen zweiten Authentifizierungsmittels vorliegt, wird dem Systemadministrator das anhand einer geeigneten Information angezeigt. Vorteilhafterweise ist jedem in der Datei enthaltenen verifizierten zweiten Authentifizierungsmittel eine dafür spezifische
15 Identifikationsinformation zugeordnet. Es kann sich dabei beispielsweise um den Namen und ggf. die Zugehörigkeit des Systemtechnikers zu einer bestimmten Organisation handeln. Im Falle einer Übereinstimmung des zweiten Authentifizierungsmittels mit einem der in der Datei
20 hinterlegten verifizierten zweiten Authentifizierungsmittel können dem Systemadministrator also zusätzlich der Name und die Organisation des Systemtechnikers angezeigt werden.

In einem besonders einfachen Fall handelt es sich beim ersten
25 und/oder zweiten Authentifizierungsmittel um einen, vorzugsweise mittels einer an einer Datenverarbeitungseinheit vorgesehenen Tastatur, an das Authentifizierungsprogramm übergebaren Authentifizierungscode. Zur Erhöhung der Sicherheit ist es zweckmäßig, dass der Authentifizierungscode
30 in einer mobilen, mit der Datenverarbeitungsanlage zur Datenübertragung verbindbaren Speichereinheit gespeichert ist. Bei der Speichereinheit kann es sich um eine mit einem Datenträger versehene Authentifizierungskarte handeln. Die Authentifizierungskarte kann ein Speichermittel, insbesondere
35 zum Speichern der Protokolldatei und/oder eine den Zugriff auf die Protokolldatei ermöglichenden Information, aufweisen. Bei der Information kann es sich beispielsweise um einen

"Link" handeln, anhand dessen die Protokolldatei aufgefunden und geöffnet werden kann.

5 Zur Erhöhung der Sicherheit kann das Freischalten einer
Zugangsberechtigung durch den Systemadministrator durch
manuelles Auslösen einem im Authentifizierungsprogramm dafür
vorgesehenen und ausschließlich dem Systemadministrator
zugänglichen Funktion erfolgen. Damit ist sichergestellt,
10 dass ein Zugriff nur mit aktiver Zustimmung des
Systemadministrators erfolgt. Es kann aber auch sein, dass
der Zugriff nach einer automatischen Prüfung des zweiten
Authentifizierungsmittels dem Systemtechniker automatisch
eingeräumt wird. Auch in diesem Fall wird erfindungsgemäß
15 automatisch insbesondere eine Protokolldatei erstellt. Das
ermöglicht einen Zugriff auf Datenverarbeitungsanlagen,
insbesondere in Krankenhäusern, die ununterbrochen
funktionsbereit gehalten werden müssen.

20 Nach einer weiteren Ausgestaltung ist vorgesehen, dass die
Verbindung zwischen der ersten und der zweiten
Datenverarbeitungseinheit über das Internet oder ein Intranet
hergestellt wird. Das ermöglicht einen Zugriff des
Systemtechnikers von einer entfernt vorgesehenen zweiten
Datenverarbeitungseinheit. Es ist somit möglich, dass ein für
25 die jeweilige Problemstellung optimal qualifizierter
Systemtechniker jederzeit, d. h. unabhängig von seinem
Aufenthaltsort, auf die Datenverarbeitungsanlage zugreifen
kann. Das ermöglicht eine schnelle und effektive Beseitigung
von Funktionsstörungen. Gleichzeitig wird dabei die
30 Authentizität des zugreifenden Systemtechnikers
sichergestellt und dessen Tätigkeit protokolliert. Der
Zugriff des Systemtechnikers erfolgt auch in diesem Fall nach
dem Grundsatz des 4-Augen-Prinzips. Mittels der
Datenverarbeitungsanlage werden insbesondere Daten
35 verarbeitet, welche einer einzelnen Person nur mit besonderer
Berechtigung oder bei Nichtvorliegen der besonderen
Berechtigung nur Personen mit einer einfachen Berechtigung

nach dem 4-Augen-Prinzip zugänglich gemacht werden dürfen. Die besondere Berechtigung wird zweckmäßigerweise durch Übergabe eines der Person zugewiesenen dritten Authentifizierungsmittels an die Datenverarbeitungsanlage nachgewiesen. Bei der einzelnen Person mit besonderer Berechtigung kann es sich beispielsweise um einen Arzt handeln. Bei den Daten kann es sich um schutzbedürftige personenbezogene Daten, insbesondere Patientendaten, handeln.

10 Nachfolgend wird ein Ausführungsbeispiel der Erfindung anhand der Zeichnung näher erläutert. Es zeigen:

Fig. 1 das Verfahren anhand einer schematischen Übersicht und

15

Fig. 2 die wesentlichen Bestandteile eines Authentifizierungsprogramms.

Fig. 1 zeigt schematisch eine erste Datenverarbeitungseinheit 1, z. B. einen Personalcomputer. Die erste Datenverarbeitungseinheit 1 ist Bestandteil einer ersten vernetzten Datenverarbeitungsanlage D1, welche als weitere Datenverarbeitungseinheiten z. B. computergesteuerte Geräte 2 oder weitere Personalcomputer 3 umfasst. Die erste Datenverarbeitungseinheit 1 ist einem Systemadministrator 4 zugewiesen, der die Datenhoheit über die erste Datenverarbeitungsanlage D1 inne hat. Der Systemadministrator 4 ist insbesondere dazu berechtigt, mittels eines ersten Programms 5 Benutzern der ersten Datenverarbeitungsanlage D1 Rollen und Rechte zuzuweisen. Derartige Rollen und Rechte ermöglichen dem jeweiligen Benutzer lediglich Zugang zu den für seinen Arbeitsbereich notwendigen Daten. Die Benutzer können auf solchen Daten jederzeit Zugreifen, d. h. auch wenn der Systemadministrator 4 nicht in die erste Datenverarbeitungsanlage D1 eingeloggt ist.

Die erste Datenverarbeitungsanlage D1 ist über eine mit einer Firewall 6 gesicherte Datenleitung 7 mit einer zweiten Datenverarbeitungsanlage D2 einer Serviceorganisation verbunden. Die Verbindung kann beispielsweise über das Internet oder ein Intranet hergestellt werden. Die zweite Datenverarbeitungsanlage D2 umfasst eine zweite Datenverarbeitungseinheit 7, z. B. einen Personalcomputer, die einem Systemtechniker 8 zugewiesen ist.

Der Systemadministrator 4 besitzt zu seiner Authentifizierung eine erste Speicherkarte 9, auf der ein erster Authentifizierungscode gespeichert ist. Der erste Authentifizierungscode kann mittels eines geeigneten Lesegeräts der ersten Datenverarbeitungsanlage D1 zum Auslesen bereitgestellt werden. Der Systemtechniker 8 besitzt zu seiner Authentifizierung eine zweite Speicherkarte 10, auf der ein zweiter Authentifizierungscode gespeichert ist. Mittels eines geeigneten Lesegeräts kann der zweite Authentifizierungscode ausgelesen und der ersten Datenverarbeitungsanlage D1 zugänglich gemacht werden. Die Leseeinheit zum Auslesen der zweiten Speicherkarte 10 muss dabei nicht unbedingt Bestandteil der ersten Datenverarbeitungsanlage D1 sein. Sie kann auch Bestandteil der zweiten Datenverarbeitungsanlage D2 sein. In diesem Fall kann die Authentizität des zweiten Authentifizierungscodes mittels eines zweiten bei der zweiten Datenverarbeitungsanlage D2 vorgesehenen Programms 11 vor dem Versuch eines Zugriffs auf die erste Datenverarbeitungsanlage D1 geprüft werden.

Die Funktion der Vorrichtung ist folgende:

Zunächst schließen ein für die erste Datenverarbeitungsanlage D1 verantwortlicher IT-Manager 12 und eine Serviceorganisation bzw. der Systemtechniker 8 einen Servicevertrag ab. Nach Abschluss eines solchen Servicevertrags erhält der Systemtechniker 8 vom IT-Manager

12 eine zweite Speicherkarte 10, auf welcher der zweite Authentifizierungscode gespeichert ist.

Bei einem ersten Wartungs-/Reparaturfall fordert der System-
5 administrator 4 mittels Telefonanruf oder per E-Mail eine Serviceleistung vom Servicetechniker 8 ab. Dabei kann es sich um eine Serviceleistung handeln, die von der zweiten Datenverarbeitungseinheit 7 aus erledigt werden kann. In diesem Fall übergibt der Servicetechniker 8 die zweite
10 Speicherkarte 10 an ein bei der zweiten Datenverarbeitungseinheit 7 vorgesehenes Lesegerät. Infolgedessen wird der den Servicetechniker 8 authentifizierende zweite Authentifizierungscode innerhalb der zweiten Datenverarbeitungsanlage D2 an das zweite
15 Programm 11 übermittelt. Der zweite Authentifizierungscode wird geprüft. Sofern das zweite Programm 11 den zweiten Authentifizierungscode als authentisch erkennt, wird über die Datenleitung 7 eine Verbindung zur ersten Datenverarbeitungsanlage D1 hergestellt. Mittels des ersten
20 Programms 5 wird der gewünschte Zugriff geprüft. Dazu wird zunächst geprüft, ob die erste Speicherkarte 9 in einem Lesegerät, z. B. bei der ersten Datenverarbeitungseinheit 1, eingesteckt ist. Sofern das nicht der Fall ist, wird ein Zugriff durch den Systemtechniker 8 nicht ermöglicht. Sofern
25 ein Zugriff auf den auf der ersten Speicherkarte 9 gespeicherten ersten Authentifizierungscode zur Authentifizierung des Systemadministrators 4 möglich ist, wird der zweite Authentifizierungscode mit einer Mehrzahl von in einer Datei gespeicherten zweiten Authentifizierungscodes
30 verglichen. Sofern der zweite Authentifizierungscode als nicht authentisch erkannt wird, wird ein Zugang für den Systemtechniker 8 nicht ermöglicht. Sofern der zweite Authentifizierungscode als authentisch erkannt wird, wird eine Protokollfunktion ausgelöst. Gleichzeitig erhält der
35 Systemtechniker 8 Zugriff auf die erste Datenverarbeitungsanlage D1. Solange der Servicetechniker 8 auf die erste Datenverarbeitungsanlage D1 zugreift, werden

sämtliche Änderungen, Ergänzungen und dgl. am Datenbestand der ersten Datenverarbeitungsanlage D1 protokolliert. Sobald der Systemtechniker 8 seine Tätigkeit abgeschlossen und sich ausgeloggt hat, wird die Protokolldatei geschlossen.

5

Die Protokolldatei enthält neben dem Protokoll über sämtliche Änderungen, Ergänzungen und dgl. am Datenbestand der ersten Datenverarbeitungsanlage D1 vorteilhafterweise zusätzlich die folgenden Informationen:

10

- Name des Systemtechnikers,

- Name der Serviceorganisation,

15

- Login-/Logout-Zeit,

- Art des Zugangs, ggf. Identifikation der zum Zugang verwendeten Datenverarbeitungseinheit.

20 Bei einem zweiten Wartungs-/Reparaturfall fordert der Systemadministrator mittels des Telefonanrufs oder per E-Mail eine Serviceleistung vom Servicetechniker 8 an, welche vor Ort auszuführen ist. Es kann sich dabei z. B. um einen Austausch eines Moduls bei einem Röntgen-Computertomografen in einem

25

Krankenhaus handeln. In diesem Fall loggt sich der Servicetechniker 8 an einer geeigneten

Datenverarbeitungseinheit der ersten Datenverarbeitungsanlage D1 unter Verwendung der zweiten Speicherkarte 10 ein. Ein Zugriff ist auch in diesem Fall nur dann möglich, wenn

30

gleichzeitig der Systemadministrator 4 unter Verwendung der ersten Speicherkarte 9 bei der ersten Datenverarbeitungsanlage D1 eingeloggt ist.

Nach einer weiteren vorteilhaften Funktion kann der

35

Systemadministrator 4 jederzeit die Tätigkeit des Systemtechnikers 8 unterbrechen, indem er einen Zugriff auf die erste Datenverarbeitungsanlage D1 durch Unterbrechung des

Zugriffs auf den ersten Authentifizierungscode unterbricht.
Das kann z. B. dadurch erfolgen, dass der Systemadministrator
4 die erste Speicherkarte 9 aus dem betreffenden Lesegerät
herausnimmt. Im Gegensatz zu herkömmlichen Verfahren behält
5 nach dem erfindungsgemäßen Verfahren der Systemadministrator
4 also stets die Datenhoheit. Außerdem ist es anhand der
automatischen Protokollierungsfunktion möglich, sämtliche
Tätigkeiten des Systemtechnikers 8 nachzuvollziehen. Im Falle
eines Missbrauchs kann ein weiterer Zugriff vom
10 Systemadministrator 8 auf die erste Datenverarbeitungsanlage
D1 ohne weiteres gesperrt werden. Dazu muss lediglich der in
der Datei gespeicherte betreffende zweite
Authentifizierungscode entfernt oder geändert werden.

15 Mit dem vorgeschlagenen Verfahren ist ein Zugriff des
Systemtechnikers 8 auf den Datenbestand der ersten
Datenverarbeitungsanlage D1 nur nach dem 4-Augen-Prinzip
möglich, d. h. ein solcher Zugriff erfolgt stets unter der
Kontrolle des Systemadministrators 4. Insoweit kann ein
20 unbefugter Zugriff des Systemtechnikers 8 auf
schutzbedürftige personenbezogene Daten, z. B.
Patientendaten, unterbunden werden.

Fig. 2 zeigt schematisch die wesentlichen Bestandteile des
25 ersten Programms 5. Mit UI1 ist eine erste
Benutzerschnittstelle zum Zugriff von der ersten
Datenverarbeitungsanlage D1 und mit UI2 eine zweite
Benutzerschnittstelle zum Zugriff z. B. über die Datenleitung
7 bezeichnet.

30 Ein Zugriffsmodul 13 ermöglicht oder sperrt einen Zugriff für
einen Systemtechniker 8 auf die erste
Datenverarbeitungsanlage D1. Das Zugriffsmodul 13 verwaltet
und vergleicht insbesondere Authentifizierungscodes.

35 Vorteilhafterweise kann das erste Programm 5 weitere Module
aufweisen, welche insbesondere Wartungs- und/oder

Reparaturarbeiten an der ersten Datenverarbeitungsanlage D1 erleichtern. So kann z. B. ein Lokalisierungsmodul 14 vorgesehen sein, mit dem festgestellt werden kann, an welcher Datenverarbeitungseinheit ein qualifizierter Systemtechniker
5 8 gerade tätig und ggf. abrufbar ist.

Mit dem Protokollierungsmodul 15 wird eine Protokollierung der Tätigkeit des Systemtechnikers 8 bewirkt. Mit dem Protokollierungsmodul 15 werden insbesondere Protokolldateien
10 erstellt und an einem vorgegebenen Ort abgelegt.

Ein Anonymisierungsmodul 16 dient insbesondere dazu, schutzbedürftige persönliche Daten zu anonymisieren. So können z. B. Namen von Patienten durch Kennziffern ersetzt
15 werden, um einen Systemtechniker 8 entsprechend den Datenschutzvorschriften einen Einblick in persönliche Daten unmöglich zu machen.

Mit Hilfsmodulen 17, 18 wird eine Beschreibung der für den Systemadministrator 4 und den Systemtechniker 8 notwendigen Funktionen des ersten Programms 5 bereitgestellt. Ein Modalitätsmodul 19 ermöglicht einen Datenaustausch, z. B. mit computergesteuerten Geräten, wie Röntgen-Computertomografen usw.. In ähnlicher Weise ermöglicht ein IT-Systemmodul 20
20 einen Datenaustausch mit Datenbanken etc.
25

Ein Betriebssystemmodul 21 schafft die notwendigen Voraussetzungen für eine korrekte Einbindung des ersten Programms 5 in das jeweils benutzte Betriebssystem.

Patentanspruch

1. Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist, mit folgenden Schritten:

Bereitstellen eines ersten Authentifizierungsmittels (9) zur Authentifizierung eines Systemadministrators (4),

10

Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe des ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),

15

Bereitstellen eines zweiten Authentifizierungsmittels (10) zur Authentifizierung eines Systemtechnikers (8),

Authentifizierung des Systemtechnikers (8) an einer zweiten Datenverarbeitungseinheit (7) durch Übergabe des zweiten Authentifizierungsmittels (10) an das Authentifizierungsprogramm (5) und dadurch bedingtes automatisches Erzeugen einer den Träger des zweiten Authentifizierungsmittels (10) identifizierenden Identifikationsinformation,

25

Anzeige der Identifikationsinformation an der ersten Datenverarbeitungseinheit (1) des Systemadministrators (4) und

30

Freischalten einer Zugangsberechtigung für den Systemtechniker (8) und automatisches Auslösen einer Funktion zum Erzeugen und Speichern einer die Tätigkeit des Systemtechnikers (8) an der Datenverarbeitungsanlage (D1) protokollierenden Protokolldatei.

35

2. Verfahren nach Anspruch 1, wobei das zweite Authentifizierungsmittel (10) mittels des Authentifizierungsprogramms (5) durch Zugriff auf eine verifizierte zweite Authentifizierungsmittel (10) enthaltende
5 Datei verglichen und bei Übereinstimmung mit einem der verifizierten zweiten Authentifizierungsmittel (10) eine entsprechende Information an den Systemadministrator (4) übermittelt wird.
- 10 3. Verfahren nach Anspruch 2, wobei jedem in der Datei enthaltenen verifizierten zweiten Authentifizierungsmittel (10) eine dafür spezifische Identifikationsinformation zugeordnet ist.
- 15 4. Verfahren nach Anspruch 3, wobei die Identifikationsinformation den Namen und ggf. die Zugehörigkeit des Systemtechnikers (8) zu einer bestimmten Organisation umfasst.
- 20 5. Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist, mit folgenden Schritten:
- 25 Bereitstellen eines ersten Authentifizierungsmittels (9) zur Authentifizierung eines Systemadministrators (4),
- Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe des
30 ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),
- Bereitstellen eines zweiten Authentifizierungsmittels (10) zur Authentifizierung eines Systemtechnikers (8),
- 35 Authentifizierung des Systemtechnikers (8) an einer zweiten Datenverarbeitungseinheit (7) durch Übergabe des zweiten

Authentifizierungsmittels (10) an das
Authentifizierungsprogramm (5) und dadurch bedingtes
automatisches Erzeugen einer den Träger des zweiten
Authentifizierungsmittels (10) identifizierenden

5 Identifikationsinformation,

wobei das erste (9) und/oder das zweite
Authentifizierungsmittel (10) ein, vorzugsweise mittels einer
an einer Datenverarbeitungseinheit (1, 7) vorgesehenen
10 Tastatur, an das Authentifizierungsprogramm (5) übergebbarer
Authentifizierungscode ist,

Anzeige der Identifikationsinformation an der ersten
Datenverarbeitungseinheit (1) des Systemadministrators (4)

15 und

Freischalten einer Zugangsberechtigung für den
Systemtechniker (8) und automatisches Auslösen einer Funktion
zum Erzeugen und Speichern einer die Tätigkeit des
20 Systemtechnikers (8) an der Datenverarbeitungsanlage (D1)
protokollierenden Protokolldatei.

6. Verfahren nach Anspruch 5, wobei der
Authentifizierungscode in einer mobilen mit der
25 Datenverarbeitungsanlage (D1, D2) zur Datenübertragung
verbindbaren Speichereinheit gespeichert ist.

7. Verfahren nach Anspruch 6, wobei die Speichereinheit eine
mit einem Datenträger versehene Authentifizierungskarte (9,
30 10) ist.

8. Verfahren nach Anspruch 7, wobei die
Authentifizierungskarte (9, 10) ein Speichermittel,
insbesondere zum Speichern der Protokolldatei und/oder einer
35 den Zugriff auf die Protokolldatei ermöglichenden
Information, aufweist.

9. Verfahren zum Zugriff auf eine Datenverarbeitungsanlage (D1), welche aus miteinander zum Datenaustausch vernetzten Datenverarbeitungseinheiten (1, 2, 3) gebildet ist, mit folgenden Schritten:

5

Bereitstellen eines ersten Authentifizierungsmittels (9) zur Authentifizierung eines Systemadministrators (4),

10

Authentifizierung des Systemadministrators (4) an einer ersten Datenverarbeitungseinheit (1) durch Übergabe des ersten Authentifizierungsmittels (9) an ein Authentifizierungsprogramm (5),

15

Bereitstellen eines zweiten Authentifizierungsmittels (10) zur Authentifizierung eines Systemtechnikers (8),

20

Authentifizierung des Systemtechnikers (8) an einer zweiten Datenverarbeitungseinheit (7) durch Übergabe des zweiten Authentifizierungsmittels (10) an das Authentifizierungsprogramm (5) und dadurch bedingtes automatisches Erzeugen einer den Träger des zweiten Authentifizierungsmittels (10) identifizierenden Identifikationsinformation,

25

Anzeige der Identifikationsinformation an der ersten Datenverarbeitungseinheit (1) des Systemadministrators (4) und

30

Freischalten einer Zugangsberechtigung für den Systemtechniker (8) und automatisches Auslösen einer Funktion zum Erzeugen und Speichern einer die Tätigkeit des Systemtechnikers (8) an der Datenverarbeitungsanlage (D1) protokollierenden Protokolldatei,

35

wobei das Freischalten einer Zugangsberechtigung durch den Systemadministrator (4) durch manuelles Auslösen einer im Authentifizierungsprogramm (5) dafür vorgesehenen und

ausschließlich dem Systemadministrator (8) zugänglichen Funktion erfolgt.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei
5 mittels der Datenverarbeitungsanlage (D1) Daten verarbeitet werden, welche

einer einzelnen Person nur mit besonderer Berechtigung

10 oder

bei Nichtvorliegen der besonderen Berechtigung nur Personen mit einer einfachen Berechtigung nach dem 4-Augen-Prinzip

15 zugänglich gemacht werden dürfen.

11. Verfahren nach Anspruch 10, wobei die besondere Berechtigung durch Übergabe eines der Person zugewiesenen dritten Authentifizierungsmittels an die
20 Datenverarbeitungsanlage (D1) nachgewiesen wird.

12. Verfahren nach Anspruch 10, wobei die Daten schutzbedürftige personenbezogene Daten, insbesondere Patientendaten, sind.

25

13. Verfahren nach Anspruch 1, wobei die Verbindung zwischen der ersten (1) und der zweiten Datenverarbeitungseinheit (7) über das Internet oder ein Intranet hergestellt wird.

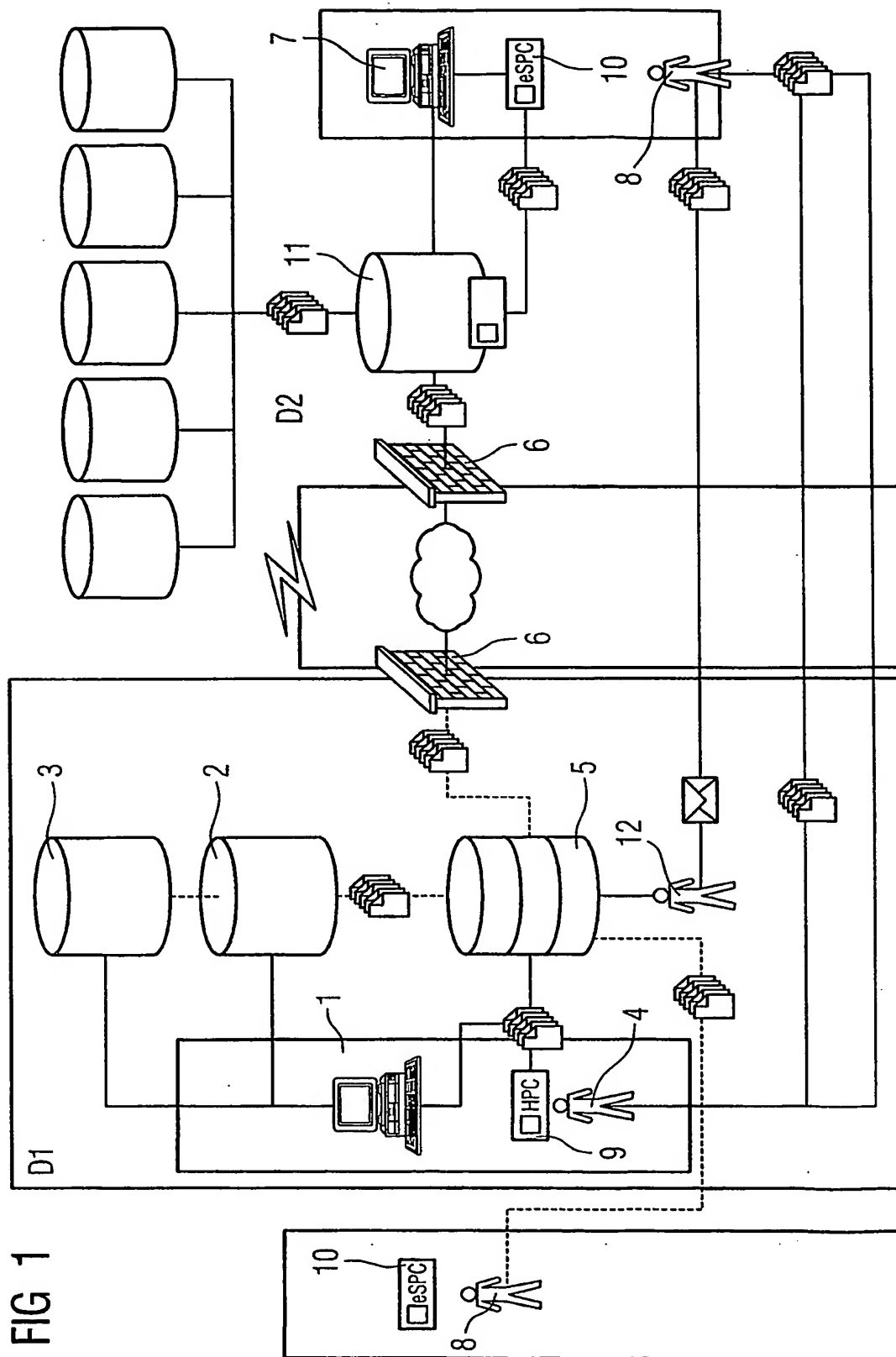
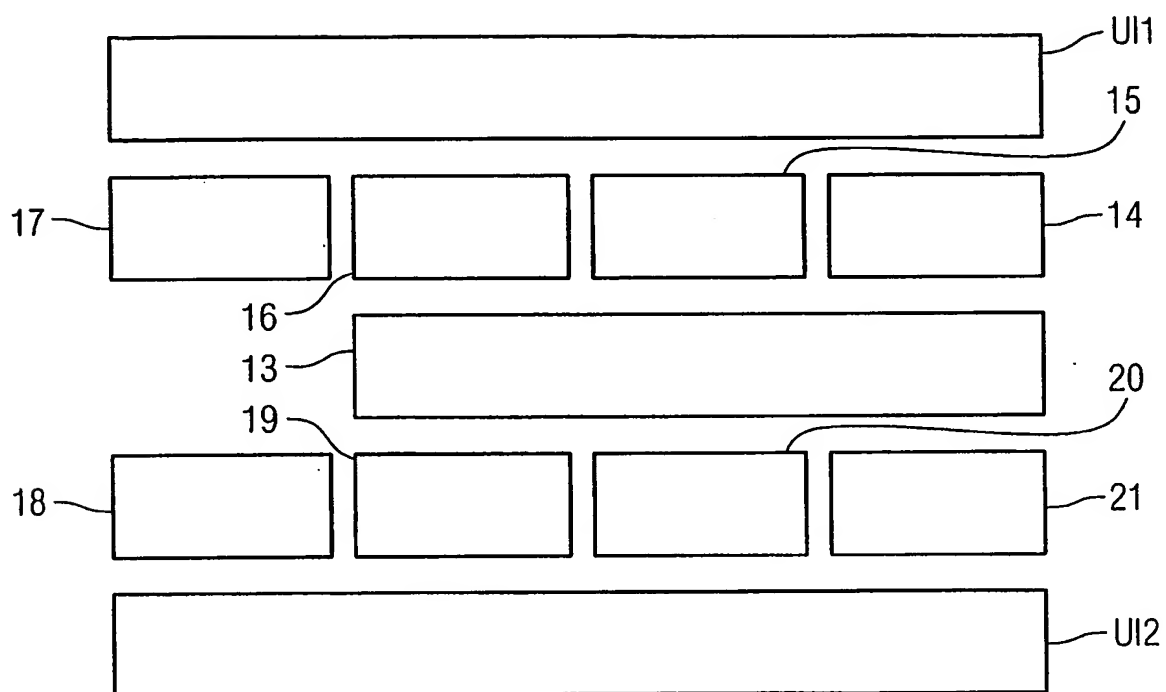


FIG 2



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP2004/052890

| A. CLASSIFICATION OF SUBJECT MATTER IPC 7 G06F1/00 | | | | |
|---|---|--|---|---|
| According to International Patent Classification (IPC) or to both national classification and IPC | | | | |
| B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 G06F | | | | |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched | | | | |
| Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal | | | | |
| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | | | |
| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. | | |
| X | DE 101 21 819 A1 (ROSNER, WOLFGANG) 21 November 2002 (2002-11-21) cited in the application abstract paragraph '0065! - paragraph '0066! paragraph '0069! - paragraph '0074! paragraph '0092! - paragraph '0095! paragraph '0102! paragraph '0119! - paragraph '0122! paragraph '0137! claims 1,3,20 | 1-13 | | |
| A | US 5 610 981 A (MOONEY ET AL) 11 March 1997 (1997-03-11) abstract column 2, line 21 - column 3, line 14 column 6, line 29 - line 40 column 11, line 13 - line 57 ----- -/-- | 1-13 | | |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. | | | | |
| <input checked="" type="checkbox"/> Patent family members are listed in annex. | | | | |
| * Special categories of cited documents: <table border="0"> <tr> <td> *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed </td> <td> *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family </td> </tr> </table> | | | *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed | *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family |
| *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed | *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family | | | |
| Date of the actual completion of the international search 24 February 2005 | | Date of mailing of the international search report 08/03/2005 | | |
| Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016 | | Authorized officer Kleiber, M | | |

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052890

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|---|-----------------------|
| A | <p>GEIGER U: "Generationswechsel bei Bildschirmschreibern" SPS MAGAZIN, CHNIK-DOKUMENTATIONS VERLAG, MARBURG, TE, vol. 2002, no. 8, August 2002 (2002-08), pages 1-2, XP002302406 ISSN: 0935-0187 the whole document</p> | 1-13 |
| A | <p>RANKL W ET AL: "Handbuch der Chipkarten, PASSAGE" HANDBUCH DER CHIPKARTEN. AUFBAU - FUNKTIONSWEISE - EINSATZ VON SMART CARDS, MUENCHEN : CARL HANSER VERLAG, DE, 1999, pages 450-459, XP002268702 ISBN: 3-446-21115-2 the whole document</p> | 1-13 |

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/EP2004/052890

| Patent document cited in search report | | Publication date | Patent family member(s) | Publication date |
|---|----|---------------------|----------------------------|---------------------|
| DE 10121819 | A1 | 21-11-2002 | NONE | |
| US 5610981 | A | 11-03-1997 | US 5327497 A | 05-07-1994 |
| | | | AT 175505 T | 15-01-1999 |
| | | | AU 703856 B2 | 01-04-1999 |
| | | | AU 2092695 A | 25-09-1995 |
| | | | BR 9506968 A | 01-06-1999 |
| | | | CA 2183759 A1 | 14-09-1995 |
| | | | CN 1146813 A | 02-04-1997 |
| | | | DE 69507129 D1 | 18-02-1999 |
| | | | DE 69507129 T2 | 05-08-1999 |
| | | | EP 0748474 A1 | 18-12-1996 |
| | | | NZ 282954 A | 24-11-1997 |
| | | | OA 10588 A | 22-08-2002 |
| | | | WO 9524696 A2 | 14-09-1995 |
| | | | AU 681588 B2 | 04-09-1997 |
| | | | AU 4528293 A | 30-12-1993 |
| | | | CA 2137274 A1 | 09-12-1993 |
| | | | EP 0643858 A1 | 22-03-1995 |
| | | | JP 7508604 T | 21-09-1995 |
| | | | WO 9324906 A1 | 09-12-1993 |
| | | | US 5515440 A | 07-05-1996 |

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/052890

| A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES IPK 7 G06F1/00 | | |
|---|--|--|
| Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK | | |
| B. RECHERCHIERTE GEBIETE Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) IPK 7 G06F | | |
| Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen | | |
| Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal | | |
| C. ALS WESENTLICH ANGESEHENE UNTERLAGEN | | |
| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
| X | DE 101 21 819 A1 (ROSNER, WOLFGANG) 21. November 2002 (2002-11-21) in der Anmeldung erwähnt Zusammenfassung Absatz '0065! - Absatz '0066! Absatz '0069! - Absatz '0074! Absatz '0092! - Absatz '0095! Absatz '0102! Absatz '0119! - Absatz '0122! Absatz '0137! Ansprüche 1,3,20 | 1-13 |
| A | US 5 610 981 A (MOONEY ET AL) 11. März 1997 (1997-03-11) Zusammenfassung Spalte 2, Zeile 21 - Spalte 3, Zeile 14 Spalte 6, Zeile 29 - Zeile 40 Spalte 11, Zeile 13 - Zeile 57 | 1-13 |
| -/- | | |
| <input checked="" type="checkbox"/> Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen | | <input checked="" type="checkbox"/> Siehe Anhang Patentfamilie |
| * Besondere Kategorien von angegebenen Veröffentlichungen : *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist | | *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindertischer Tätigkeit beruhend betrachtet werden *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindertischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist *Z* Veröffentlichung, die Mitglied derselben Patentfamilie ist |
| Datum des Abschlusses der Internationalen Recherche 24. Februar 2005 | | Absenddatum des Internationalen Recherchenberichts 08/03/2005 |
| Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016 | | Bevollmächtigter Bediensteter Kleiber, M |

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/052890

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|------------|--|--------------------|
| A | <p>GEIGER U: "Generationswechsel bei Bildschirmschreibern" SPS MAGAZIN, CHNIK-DOKUMENTATIONS VERLAG, MARBURG, TE, Bd. 2002, Nr. 8, August 2002 (2002-08), Seiten 1-2, XP002302406 ISSN: 0935-0187 das ganze Dokument</p> | 1-13 |
| A | <p>RANKL W ET AL: "Handbuch der Chipkarten, PASSAGE" HANDBUCH DER CHIPKARTEN. AUFBAU - FUNKTIONSWEISE - EINSATZ VON SMART CARDS, MUENCHEN : CARL HANSER VERLAG, DE, 1999, Seiten 450-459, XP002268702 ISBN: 3-446-21115-2 das ganze Dokument</p> | 1-13 |

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2004/052890

| Im Recherchenbericht angeführtes Patentdokument | | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | | Datum der Veröffentlichung |
|--|----|-------------------------------|-----------------------------------|-------------|-------------------------------|
| DE 10121819 | A1 | 21-11-2002 | KEINE | | |
| US 5610981 | A | 11-03-1997 | US | 5327497 A | 05-07-1994 |
| | | | AT | 175505 T | 15-01-1999 |
| | | | AU | 703856 B2 | 01-04-1999 |
| | | | AU | 2092695 A | 25-09-1995 |
| | | | BR | 9506968 A | 01-06-1999 |
| | | | CA | 2183759 A1 | 14-09-1995 |
| | | | CN | 1146813 A | 02-04-1997 |
| | | | DE | 69507129 D1 | 18-02-1999 |
| | | | DE | 69507129 T2 | 05-08-1999 |
| | | | EP | 0748474 A1 | 18-12-1996 |
| | | | NZ | 282954 A | 24-11-1997 |
| | | | OA | 10588 A | 22-08-2002 |
| | | | WO | 9524696 A2 | 14-09-1995 |
| | | | AU | 681588 B2 | 04-09-1997 |
| | | | AU | 4528293 A | 30-12-1993 |
| | | | CA | 2137274 A1 | 09-12-1993 |
| | | | EP | 0643858 A1 | 22-03-1995 |
| | | | JP | 7508604 T | 21-09-1995 |
| | | | WO | 9324906 A1 | 09-12-1993 |
| | | | US | 5515440 A | 07-05-1996 |

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☒ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.